Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

In This Issue

Quick Links

Scholarship applications dueJanuary 31, 2015

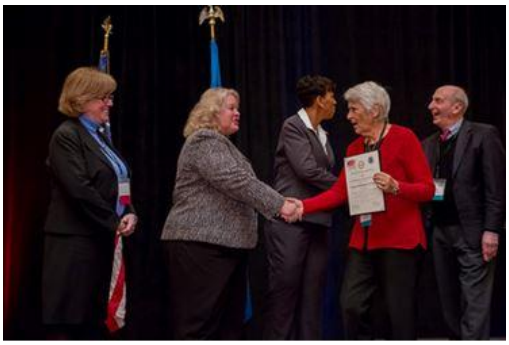
Cybersecurity is increasingly seen as an interdisciplinary field.

The CyberCorps Scholarship includes**full tuition and fees coverage, a living**

January 20, 2015

Ten (10) Cyber security Events are scheduled in the Greater Washington Area in the next few weeks.

GWU awarded funding for cybersecurity education



Dr. Joan Ferrini-Mundy, Assistant Director, National Science Foundation Directorate for Education and Human Resources; Ms Donna Seymour, Chief Information Officer, Office of Personnel Management; Ms. Renee Forney, Executive Director, Departmer of Homeland Security CyberSkills Initiative; Prof. Rachelle Helle GW; Prof. Lance Hoffman, GW

Continuing cybersecurity education

At an awards ceremony on January 12, Professors Lance Hoffman and Rachelle Heller accepted a certificate commemorating GW's 5-year renewal award of over $4,000,000 to continue educating students in cybersecurity who are committed to work for the government upon graduation.

Events

Click here for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

Remember...

The CSPRI office has moved.
We are now located in Tompkins Hall:

725 23rd Street NW
Suite 106
Washington, DC
20052

stipend for the academic year, a book allowance, and a professional development fund.

For more information on the program, click**here.**

Legislative Lowdown

-The National Journal has a useful breakdown of the White House's draft proposal for new cybersecurity legislation. The White House has dedicated much of this week to pushing a framework for cybersecurity legislation that administration officials say could shore up the nation's cyber defenses and help prevent breaches like the recent Sony hack or previous attacks on companies including Target and JP Morgan," writes Dustin Volz.
"But some analysts aren't convinced that an information-sharing proposal at the center of the push would really have done much to prevent those high-profile hacks, and could actually further threaten customers' privacy by handing over data to government agencies such as the National Security Agency." Read more here.

Cyber Security Policy News

Update: North Korea cyberattack
-The trail that led American officials to blame North Korea for the destructive cyberattack on Sony Pictures Entertainment in November winds back to 2010, when the National Security Agency scrambled to break into the computer systems of a country considered one of the most impenetrable targets on earth, The New York Timesreported last week. "Spurred by growing concern about North Korea's maturing capabilities, the American spy agency drilled into the Chinese networks that connect North Korea to the outside world, picked through connections in Malaysia favored by North Korean hackers and penetrated directly into the North with the help of South Korea and other American allies, according to former United States and foreign officials, computer experts later briefed on the operations and a newly disclosed N.S.A. document," The Times' David Sanger and Martin Fackler wrote. "A classified security agency program expanded into an ambitious effort, officials said, to place malware that could track the internal workings of many of the computers and networks used by the North's hackers, a force that South Korea's military recently said numbers roughly 6,000 people."

Obama calls for tech backdoors
-President Obama last week called on tech leaders to avoid putting in unbreakable encryption that could block law enforcement officials from lawfully using the services to investigate crimes. The Hill quotes Obama in a meeting with British Prime Minister David Cameron last week: "Social media and the Internet is the primary way in which these terrorist organizations are communicating. That's not different from anybody else, but they're good at it and when we have the ability to track that in a way that is legal, conforms with due process, rule of law and presents oversight, then that's a capability that we have to preserve."

US cybersecurity report: encryption needed

Follow Us

Follow us on Twitter:
@gwCSPRI

Follow CSPRI Director, Lance Hoffman:
@lancehoffman1

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

Follow CSPRI Research Scientist, Allan Friedman:
@allanfriedman

Meanwhile, a secret US cybersecurity report warned that government and private computers were being left vulnerable to online attacks from Russia, China and criminal gangs because encryption technologies were not being implemented fast enough, according to The Guardian. "The advice, in a newly uncovered five-year forecast written in 2009, contrasts with the pledge made by David Cameron this week to crack down on encryption use by technology companies," writes James Ball. The story notes that while U.S. and U.K. leaders are urging companies to backdoor their services for government investigators, "the document from the US National Intelligence Council, which reports directly to the US director of national intelligence, made clear that encryption was the best defense for computer users to protect private data."

NSA update

Non-stop disclosures about the U.S. government's domestic cyber surveillance activities at the National Security Agency are prompting moves by the White House to make important changes to the way the agency operates, according to the National Journal. "The Obama administration is planning to issue a series of progress updates about its efforts over the past year to reform the National Security Agency's mass-surveillance authority," Dustin Volz writes. "An announcement is expected to come by the end of the month, a White House spokesman said, and will include details about changes to the NSA's bulk collection of domestic phone records, one of the most controversial programs revealed by Edward Snowden 18 months ago. Some of that information was released Thursday in a report by the National Research Council, which concluded the use of software alone cannot entirely replace bulk surveillance."

UK and US: teaming up

-The UK and US are to carry out "war game" cyber attacks on each other as part of a new joint defense against online criminals, the BBC reports. "The first exercise, a staged attack on the financial sector, will take place later this year," writes Gordon Correra. "The 'unprecedented' arrangement between the two countries was announced by Prime Minister David Cameron ahead of talks with US President Barack Obama."

About this Newsletter

This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area. It is published by the Cyber Security Policy and Research Institute (CSPRI) of the George Washington University. CSPRI is a center for GW and the Washington area that promotes technical research and policy analysis of topics in or related to cybersecurity. More information is available at our website, http://www.cspri.seas.gwu.edu

CSPRI

202 994 5613. cspri@gwu.edu
304 Staughton Hall
707 22nd St., NW
Washington DC, DC 20052